RSAC 2025 Conference

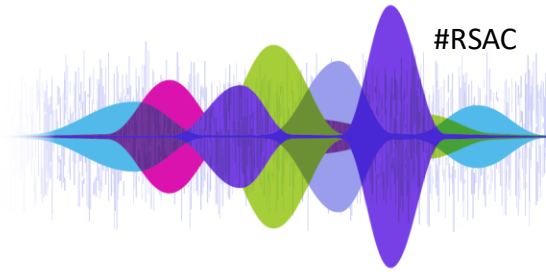
Many Voices.
One Community.

SESSION ID: SBV-R02

Demystifying CTFs

Wesley Thurner

Principal Security Engineer
Intuit / Adversary Management
https://www.linkedin.com/in/wesleythurner/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Overview

Participating in CTFs

Running your own event

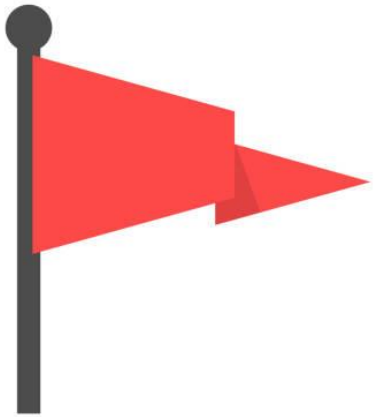
Building a CTF team

RSAC 2025 Conference

Participating in CTFs

What is a Capture the Flag (CTF)

- Gamified competition exploring different cyber security disciplines
- Each challenge has a solution measured by capturing a “flag”
- Flag formats like “flag{50me7hing_w1tty}”
- Time constrained event to solve challenges
- Creative flair



CTF Styles

- Jeopardy
  - Choose your own adventure
  - The challenges are not related to each other
  - Variety of challenge types
  - Point value aligned to difficulty

CTF Styles

- Attack and Defense
  - Offense & Defense skills required
  - First Protect your box
  - Understand the vulnerabilities they introduced
  - Patch those vulnerabilities
  - Attack those vulnerabilities on the other team's boxes

CTF Styles

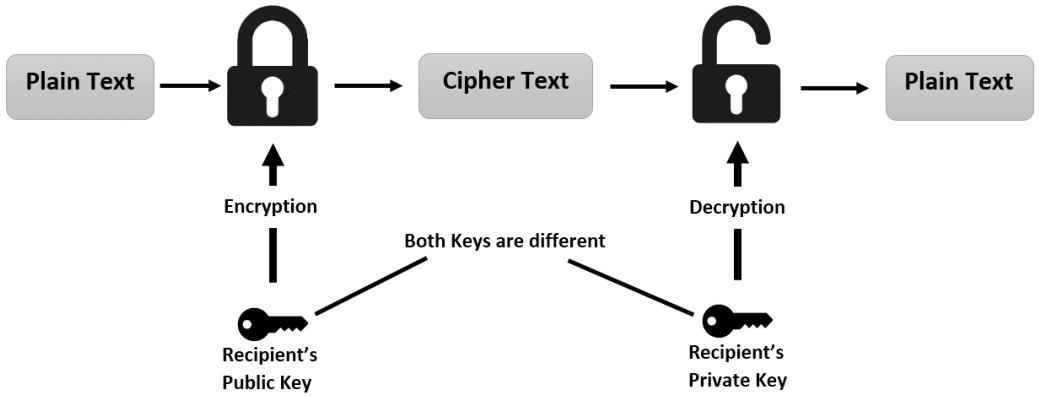
- King of the Hill
  - There will only be one winner
  - Fast paced style of play
  - Identify vulnerabilities
  - Attack the target then patch
  - Hold the target as long as possible to score points

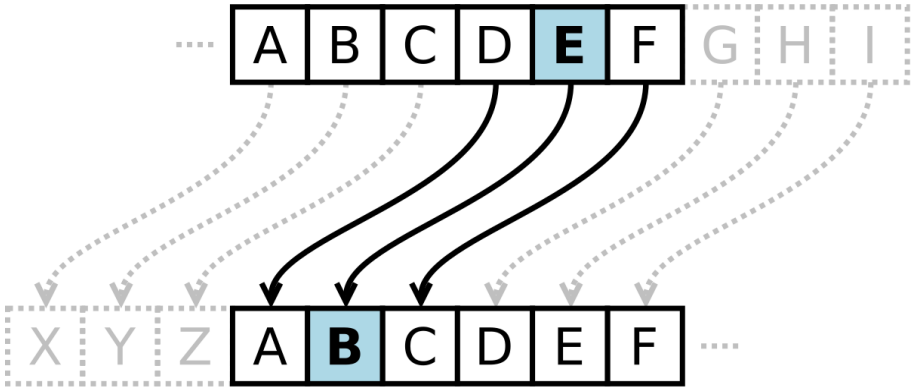
CTF Styles

- Story/Scenario Driven
  - Immersive storyline to follow
  - Variety of challenges woven into the story
  - Not a random collection of challenges
- These are the most entertaining for me

Types of Challenges

- Cryptography
  - Weakness in encryption
  - Weakness in the implementation of encryption
  - Encoding of information
  - Ceasar Ciphers
- Perfect category for developers and math majors





Types of Challenges

- Computer Exploitation
  - Recent Vulnerabilities
  - Misconfigurations
  - Zero Days
  - Credentials
- Perfect category for attackers and defenders
- Way to stay up to date

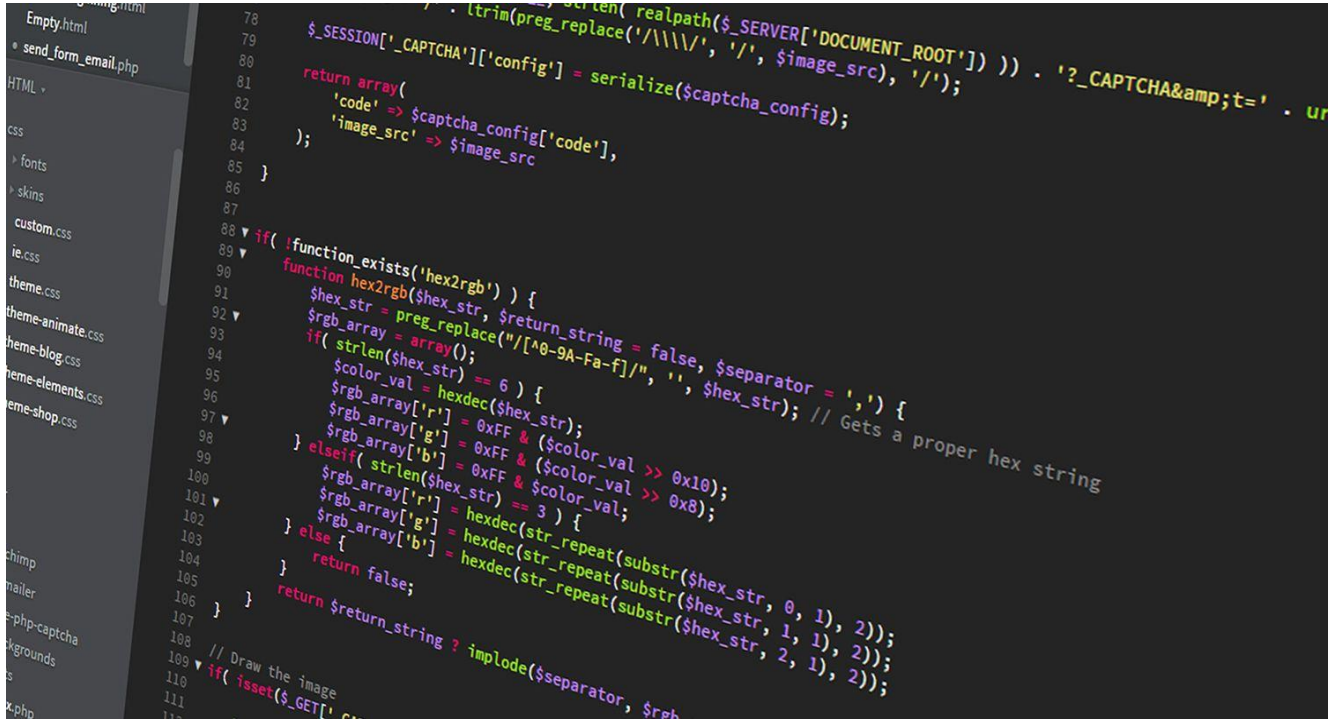
New RCE Vulnerability - CVE-2024-6409

Types of Challenges

- Forensics
  - Disk Image from compromised HDD
  - Metadata of a file
  - Logs from a domain controller
  - PCAPs of network traffic
- Perfect category for anyone who wants to understand how systems truly work

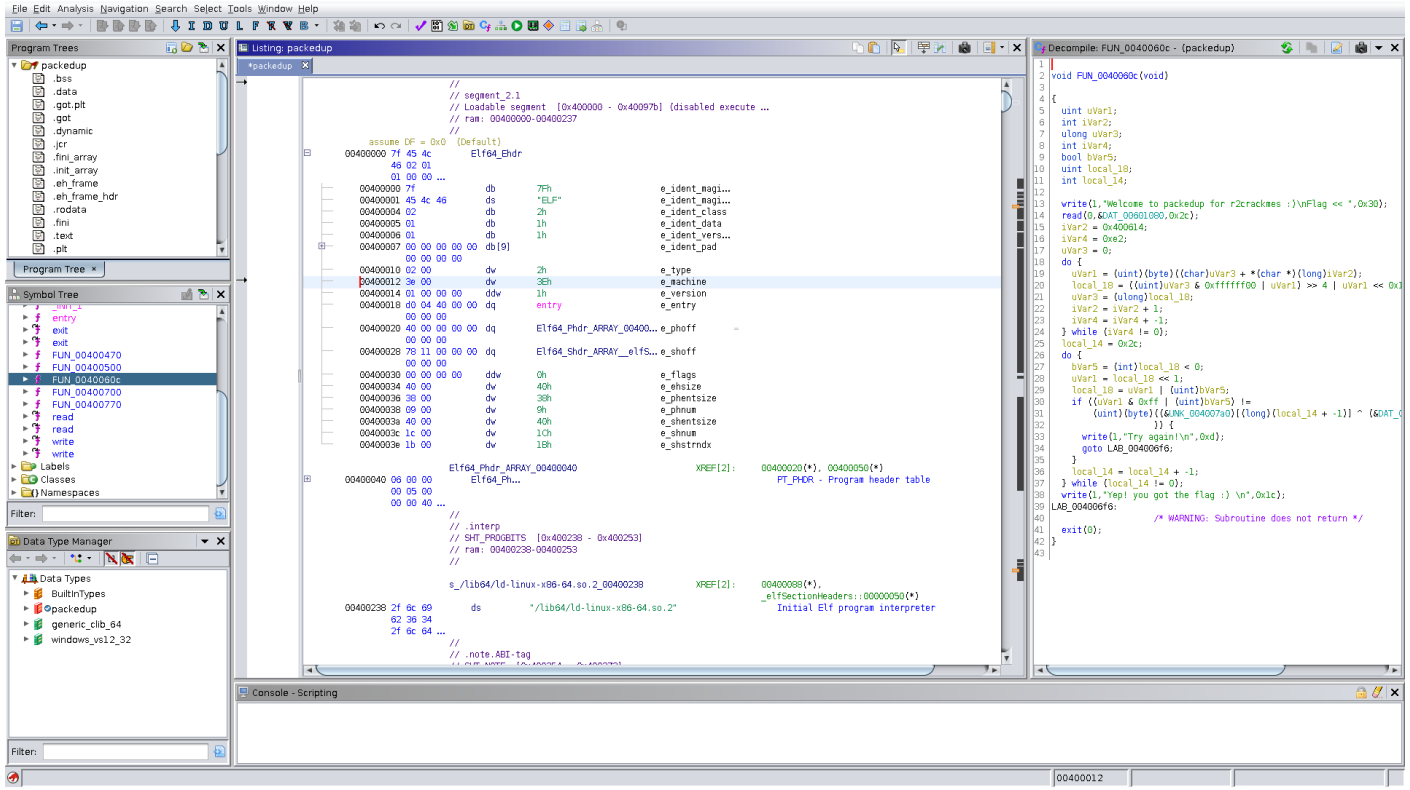
Types of Challenges

- Programming
  - Scaling manual actions
  - Time requirements
  - Advanced attacks
- Perfect category for developers or enthusiasts



Types of Challenges

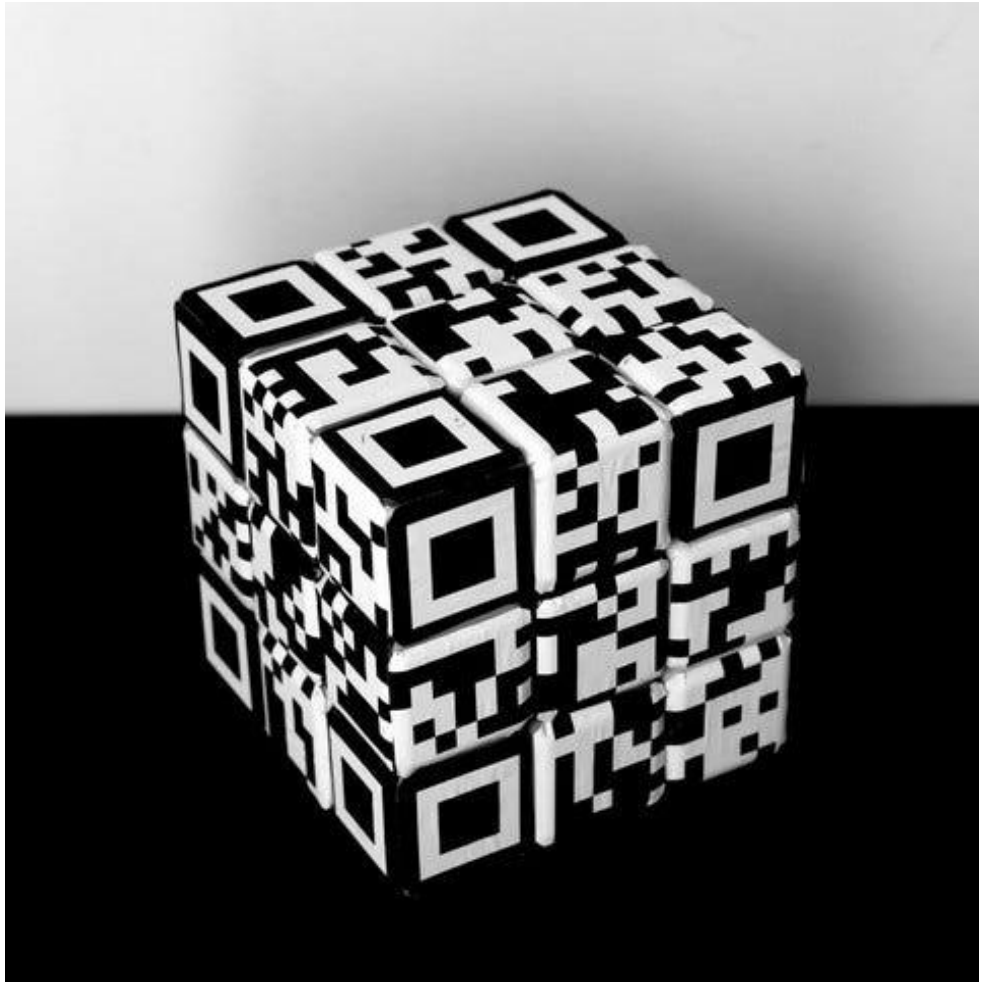
- Reverse Engineering
  - Decompile binary
  - Patch binary
  - Create exploit
  - Sometimes it is just strings
- Perfect category for low level programmers



INTUIT
turbotax creditkarma quickbooks mailchimp
RSAC 2025 Conference

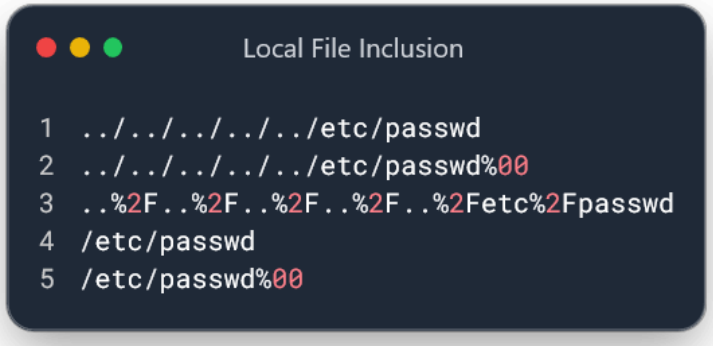
Types of Challenges

- Trivia/Puzzle
  - Author's choice
  - Very fun or frustrating
  - How many lines of code in Win XP?
- Perfect category for anyone



Types of Challenges

- Web
  - Broken Access Control
  - Misconfiguration
  - CSRF, SSRF, XSS, LFI, RFI
- Perfect category for frontend or backend developers



Types of Challenges

- Misc
  - All others fall into this category
  - Unique challenges
- For me this can be a really fun or frustrating category

Technical Skills, Tools and Techniques

WINDOWS

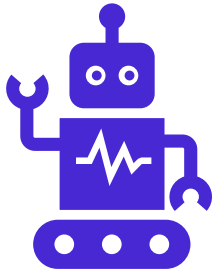
LINUX

INFRASTRUCTURE

NETWORKING

SCRIPTING

Technical Vignettes



IOT CTF

Developed tools

Cross compiled binaries

Learned a lot about IOT

Used those skills on assessments

Malware Reverse Engineering

Rudimentary skills gained through various CTFs

Used on assessments to examine unknown binaries

Non-Technical Skills

CREATIVITY

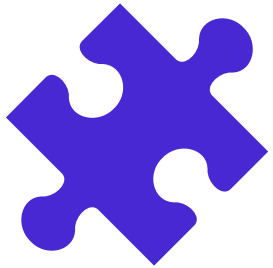
PERSISTENCE

NOTE TAKING

PREPARATION AND PRACTICE

ATTENTION TO DETAIL

Non-Technical Vignette



Geocaching/Escape rooms

Common techniques

Recognizing patterns

Scratch near a puzzle

Timestamp of binaries

Note taking is critical!

Terminal screens

Web requests

Network traffic

Proxy logs

Socializing & Teamwork

- Know your team
- Learn as a team
- Leverage the expertise of others
- Bonding
- Communicating effectively
- Knowledge sharing

Post CTF

- Blog Writeups of the challenges
- Create Video walk throughs
- Build out Tooling
- Test approaches you couldn't during the event
- Analysis and self-improvement

RSAC™ 2025 Conference

Running your event

R3DC0N at Intuit

- Internal security conference held twice a year
- Engaging CTF built by the security team
- Participants from across the company
- Experiential learning at it's best

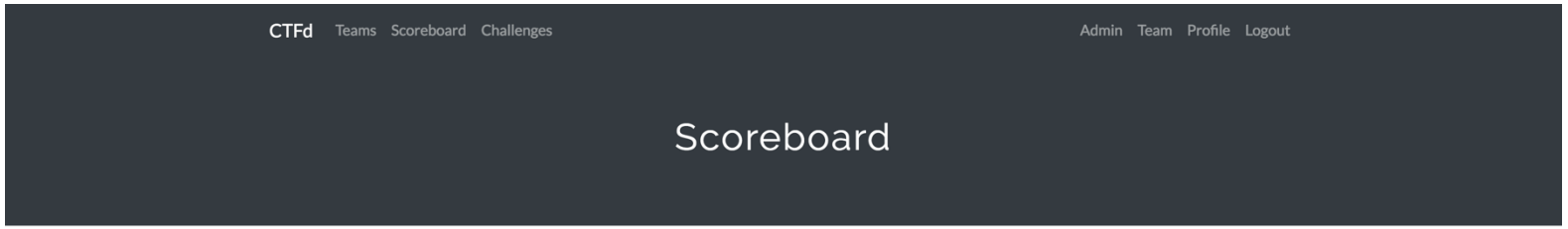
R3DC0N at Intuit

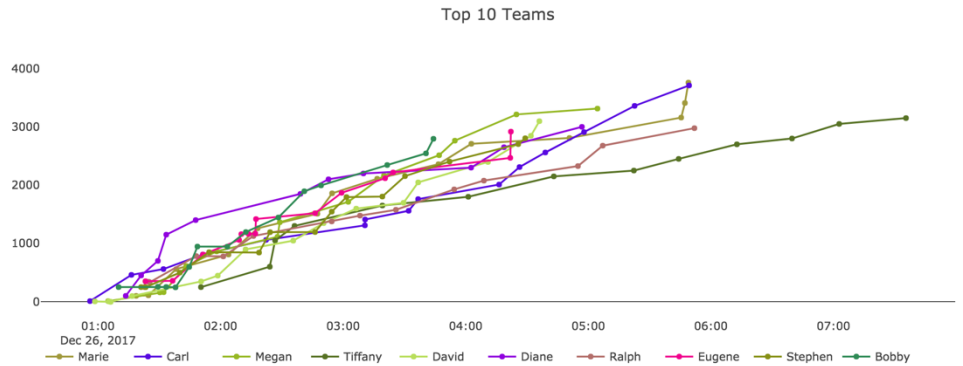
- CTF drives participation in the event
- Provides hands on activities for participants
- Teams from different departments compete
- Prizes for top teams

R3DC0N at Intuit

- 300+ players each time
- Team based
- SWEs, Marketing, PMs, SE, etc
- Beginner to advanced
- Some teams naturally form
- Pair players based on skills

CTFd





Place	Team	Score
1	Marie	3759
2	Carl	3710
3	Megan	3313
4	Tiffany	3150
5	David	3097
6	Diane	3000

Infrastructure

- Challenges usually Docker
- Kubernetes
  - Local
  - Cloud
- Some are machines/networks
  - Terraform
  - Ansible

kubernetes

Infrastructure

- Player devices?
  - Corporate laptop
  - VMs
- Protected Network Access

Value to the company

Builders

Learning and growth in creating challenges

Operating system protections

Deployment of challenges

Container orchestration

Players

Hands-on skills development

Rapid exposure to multiple disciplines

Understanding vulnerabilities

Team Collaboration

RSAC 2025 Conference

Building an Internal CTF Team

Assembling Your Team

- Diverse skillset is needed, look to complement skillsets
  - Web
  - Reverse Engineer
  - Crypto
  - Programmer
- Practice as a team is crucial
  - Play through completed events with writeups
  - Build the cohesiveness of the team through practice and events
  - Train together to learn limitations

Finding Events

- In person
  - Travel to larger events, but can be costly
  - Local events like BSides and meetups
- Virtually
  - Use CTFTime.org to find events

Marketing

- Build a security brand through reputation
  - Paranoids
  - Project Zero
- Sponsoring Conferences
  - If you are already traveling to an event you could also sponsor one
  - A booth at conference can be used for multiple marketing, recruitment, players

Recruitment

- Identify talent
  - Rapidly assess skills challenging environments
  - Team fit in stressful environments
  - Hidden talent – not everyone who is interested is a security engineer

RSAC 2025 Conference

Conclusion

“Apply” Slide

- Next week you should:
  - Search for open CTFs that interest you!
  - Find others within your company that are interested and recruit them.
- In the first three months following this presentation you should:
  - Solidify your CTF team
  - Sharpen your skills by trying different types of CTFs
  - Refine your process as you challenge yourself
  - Start to build a CTF internally for practice

“Apply” Slide

- Within six months you should:
  - Feel comfortable applying your skills from CTFs to your technical work
  - Identify events for your team to participate in
  - Host an internal event with the CTF challenges you built
  - Build a plan for the company to sponsor the team and market
- Within a year you should:
  - Your CTF team have participated in a public event
  - Networked with other CTF players

RSAC™ | 2025 Conference

Many Voices.
One Community.